IN THE CLAIMS

Please substitute claims 1-31 with the following:

1. (Currently Amended) A content distribution system for performing content transaction management utilizing an encrypted data packet in the form of a secure container, comprising:

a content provider which generates the secure container including a first section and a second section;

a plurality of user devices configured to receive the secure container from the content provider ~~among which the content transaction management allows a content to be secondarily distributed~~; and

the ~~a~~ secure container ~~containing the content encrypted by a content key, and container information including conditions set for a transaction of the content:~~,

~~a first section for distributing the content by transmitting said secure container; and~~

~~a second section for performing person authentication, when said secure container is transmitted among said plurality of user devices, which includes based on a person identification certificate (hereinafter, simply referred to as an IDC) which includes a template having biometric information encrypted in one of a plurality of manners, serving as person identification data of a target user for the content transaction and which is identified in reference to an IDC identifier list,~~

wherein,

the secure container contains a content encrypted by a content key and container information including conditions relating to a transaction of the content,

the first section of the secure container contains information relating to transmitting said secure container to the plurality of user devices,

the second section of the secure container includes a person identification certificate (IDC) and an IDC identifier list to authenticate a user when said secure container is transmitted to said plurality of user devices,

the IDC includes a biometric information template encrypted in one of a plurality of manners which is identifiable in the IDC identifier list,

~~the container information includes the IDC identifier list as a list of the IDCs,~~

~~the IDC identifier list is generated by a person identification authority (hereinafter, simply referred to as an IDA) as a third party agent, and~~

one of the user devices is a secure container distributing device which ~~among said plurality of user devices~~ (1) receives a primary distribution including the secure container from the content provider and verifies the authenticity of the secure container, ~~(1)~~ (2) ~~decrypts~~ decrypts and extracts the encrypted biometric information template stored in the IDC ~~identified in reference to the IDC identifier list based on the one of the plurality of manners~~ and ~~(2)~~ (3) is configured to ~~(a)~~ compare sampling information input by a user of a receiving device which is one of the user devices with the decrypted biometric information template to ~~process person authentication of~~ authenticate the [[a]] user of [[a]] the receiving device, ~~which is device a receiving device among said plurality of user devices, to which the secure container is to be distributed, and to (b)~~ perform a process of distribution of

the secure container distributing device initiates a secondary distribution after the primary distribution by sending the content key to the receiving device, and

the receiving device ~~for decrypting~~ decrypts and copies the content ~~stored in~~ sent from said secure container distributing device, after the user of the receiving device is authenticated ~~when the comparison result is affirmative~~.

2. (Currently Amended) The content distribution system according to Claim 1, wherein ~~a secure container~~

the receiving device ~~among said plurality of user devices~~ generates usage control status information ~~on a~~ relating to the content ~~based on the container information~~ included in said secure container, and

the receiving device stores the usage control status information ~~which,~~ including the IDC identifier list in a memory of the receiving device. ~~, and further~~

~~the usage control status information includes the IDC identifier list.~~

3. (Currently Amended) The content distribution system according to Claim 1, wherein

the receiving device ~~among said plurality of user devices~~ generates usage control status information ~~on a~~ relating to the content based ~~on the container information~~ included in said secure container, and stores the usage control status information, which includes the IDC identifier list, in a memory of the receiving device, and ~~further~~

the usage control status information includes conditions ~~set for~~ relating to processing the secondary distribution of the content after ~~a~~ the primary content distribution.

4. (Currently Amended) The content distribution system according to Claim 1, wherein ~~a~~

the secure container distributing device ~~among said plurality of user devices~~ is configured to authenticate the user of the receiving device by ~~compare~~ comparing sampling information

input by a user of the receiving device with the biometric information template, and ~~stored in the IDC identified in reference to the IDC identifier list, to process person authentication of a user of a receiving device among said plurality of user devices, to which the secure container is to be distributed, and to perform a process so that a~~

the secure container distributing device makes the content ~~is~~ available ~~at~~ to the receiving device, ~~when the comparison result is affirmative~~ after the user of the receiving device is authenticated.

5. (Cancelled).

6. (Currently Amended) The content distribution system according to Claim 1, wherein ~~a~~

the secure container distributing device ~~among said plurality of user devices~~ is configured to authenticate ~~a~~ the user of the receiving device by comparing ~~compare~~ sampling information input by a user of the receiving device with the biometric information template ~~stored in the IDC identified in reference to the IDC identifier list, to process person authentication of~~ authenticate ~~a the user of the receiving device, to which the secure container is to be distributed, and~~

the secure container distributing device ~~to notify a distributing device among said user devices, as a distributor of said secure container,~~ notifies the content provider of the ~~process~~ authentication result ~~of the person authentication~~, and ~~further~~

the secure container distributing device is configured to ~~perform a process so that a~~ make the content ~~is~~ available ~~at~~ to the receiving device, ~~when the comparison result is affirmative~~ after the user of the receiving device is authenticated.

7. (Currently Amended) The content distribution system according to Claim 1, wherein ~~a~~

the secure container distributing device ~~among said plurality of user devices~~ is configured to authenticate a user of the receiving device by ~~compare~~ comparing sampling information input by a user of the receiving device with the template stored in the IDC, ~~identified in reference to the IDC identifier list, to process person authentication of a user of the receiving device, to which the secure container is to be distributed,~~ and

the secure container distribution device ~~to notify a the distributing device among said user devices, as a distributor of said secure container,~~ notifies the content provider of the ~~process~~ authentication result ~~of the person authentication~~, and ~~further~~

the distributing device is configured to ~~perform processes so that~~ distribute said secure container and said content key stored in said secure container ~~are distributed~~ to the receiving device ~~of said secure container~~ and to make the secure container available at the receiving device, ~~when the comparison result is affirmative~~ after the user of the receiving device is authenticated.

8. (Currently Amended) The content distribution system according to Claim 1, wherein the IDC ~~used for person authentication, which is performed when said secure container is transmitted among said plurality of user devices,~~ is ~~configured to be~~ stored in advance ~~in~~ on any of said plurality of user devices which ~~is to perform the person~~ performs authentication.

9. (Currently Amended) The content distribution system according to Claim 1, wherein any of said user devices ~~, which is to perform person authentication when said~~ authenticates the user of the user device transmitting the secure container ~~is transmitted among of said plurality of user devices~~, and

any of said plurality of user devices is configured to obtain the IDC ~~used for the person authentication from the IDA as an issuer of the IDCs~~.

10. (Currently Amended) The content distribution system according to Claim 1, wherein the container information ~~further~~ includes content usage permission data, ~~of the content~~, and ~~a~~

the receiving device ~~among said plurality of user devices~~ is configured to ~~perform restricting~~ restrict usage of the content based on the content usage permission data ~~of the content~~ or usage control status information ~~generated according to said content usage permission data~~.

11. (Currently Amended) The content distribution system according to Claim 1, wherein said secure container ~~further is configured to include~~ includes a digital signature of ~~a producer of~~ the device sending said secure container.

12. (Currently Amended) The content distribution system according to Claim 1, wherein the IDC identifier list ~~is configured to include~~ includes data ~~for associating~~ effective to associate a user identifier with his/her IDC identifier.

13. (Currently Amended) The content distribution system according to Claim 1, wherein ~~each of~~ the content provider, the secure container distributing device and the receiving devices ~~among said plurality of user devices, which are to perform a content transaction, further comprises~~ include an encryption unit~~, so that each of the devices is configured~~ effective to ~~perform mutual authentication~~ mutually authenticate a data transmission ~~upon performing data transmission~~ between any two of the content provider, the secure container distributing device ~~and~~ or the receiving devices, and ~~further~~

the data transmitting and receiving sides are configured, respectively, to generate a digital signature of the transmitting data and to verify the digital signature.

14. (Currently Amended) The content distribution system according to Claim 1, wherein the biometric information template comprises at least any one of the following

fingerprint information, retina pattern information, iris pattern information, voice print information, and handwriting information.

15. (Withdrawn) A content distribution method for performing content transaction management for allowing a content to be secondarily distributed among a plurality of user devices, comprising the steps of:

distributing the content by transmitting a secure container containing the content encrypted by a content key, and container information including conditions set for a transaction of the content; and

performing personal authentication, when the secure container is transmitted among the plurality of user devices, based on an IDC which is identified in reference to an IDC identifier list,

wherein the container information contains the IDC identifier list as a list of the IDCs storing a template, each IDC serving as identification data of a target user for the content transaction.

16. (Withdrawn) The content distribution method according to Claim 15, wherein the IDC is generated by an IDA serving as a third party agent.

17. (Withdrawn) The content distribution method according to Claim 15, wherein a secure container receiving device among the plurality of user devices comprises the steps of:

generating usage control status information on a content based on the container information included in the secure container; and

storing the usage control status information in a memory of the receiving device,

besides the status information includes the IDC identifier list

18. (Withdrawn) The content distribution method according to Claim 15, wherein a secure container receiving device among the plurality of user devices comprises the steps of:

generating the usage control status information on a content based on the container information included in said secure container; and

storing the usage control status information in a memory of the receiving device, besides the usage control status information includes conditions set for processing secondary distribution of the content after a primary content distribution.

19. (Withdrawn) The content distribution method according to Claim 15, wherein a secure container distributing device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of a receiving device among the plurality of user devices, to which the secure container is to be distributed; and

performing a process so that a content is available at the receiving device, when the comparison result is affirmative.

20. (Withdrawn) The content distribution method according to Claim 15, wherein a secure container distributing device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of a receiving device among the plurality of user devices, to which the secure container is to be distributed; and

performing distribution of the content key for encrypting the content stored in the secure container, when the comparison result is affirmative.

21. (Withdrawn) The content distribution method according to Claim 15, wherein a secure container receiving device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of the receiving device, to which the secure container is to be distributed; and

notifying a distributing device among the user devices, as a distributor of said secure container, of the result of personal authentication,

besides the distributing device comprises the step of performing a process so that a content is available at the receiving device, when the comparison result is affirmative.

22. (Withdrawn) The content distribution method according to Claim 15, wherein a secure container receiving device among the plurality of user devices comprises the steps of:

comparing sampling information input by a user with the template stored in the IDC identified in reference to the IDC identifier list;

performing personal authentication of a user of the receiving device, to which the secure container is to be distributed; and

notifying a distributing device among the user devices, as a distributor of the secure container, of the result of personal authentication,

besides the distributing device comprises the step of performing distribution of the secure container and the content key stored in the secure container for encrypting the content to the receiving device of the secure container, when the comparison result is affirmative.

23. (Withdrawn) The content distribution method according to Claim 15, wherein the IDC used for personal authentication, which is performed when the secure container is transmitted among the plurality of user devices, is stored in advance in any of the plurality of user devices which is to perform the personal authentication.

24. (Withdrawn) The content distribution method according to Claim 15, wherein any of the plurality of user devices, which is to perform personal authentication when the secure container is transmitted among the plurality of user devices, comprises the step of obtaining the IDC necessary for the personal authentication from the IDA as an issuer of the IDCs.

25. (Withdrawn) The content distribution method according to Claim 15, wherein the container information further includes usage permission data of the content such as reproduction and duplication of the content, and a receiving device among the plurality of user devices comprises the step of performing restricting usage of the content based on the usage permission data of the content or the usage control status information generated according to said usage permission data.

26. (Withdrawn) The content distribution method according to Claim 15, wherein each of content transacting user devices among the plurality of user devices includes an encryption unit and comprises the step of performing mutual authentication upon performing

data transmission among the content transacting user devices, besides data transmitting and receiving sides comprise the steps of, respectively, generating a digital signature of the transmitting data and verifying the digital signature.

27. (Withdrawn) An information processing apparatus for reproducing a content stored in a storage device, comprising:

a storing section for storing the content in the apparatus when a secure container, including the content encrypted by a content key and container information containing conditions set for a sales price as well as a sales restriction of the content, is transmitted; and

a processing section for performing personal authentication based on an IDC identified in reference to an IDC identifier list when the content is regenerated,

wherein a template serves as identification data of a target user for a content transaction, and the container information includes the IDC identifier list as a list of the IDCs storing the template, each IDC being generated by an IDA serving as a third party agent.

28. (Withdrawn) The information processing apparatus according to Claim 27, wherein said processing section, further comprising:

a first processing sub-section for performing the personal authentication by comparing the template stored in the IDC identified in reference to the IDC identifier list with sampling information input by a user.

29. (Withdrawn) The information processing apparatus according to Claim 27, wherein said processing section, further comprising:

a second processing sub-section for performing the personal authentication of a user who is to be permitted to access the information processing apparatus, based on a device-dependent IDC set to the apparatus; and

a third processing sub-section for performing the personal authentication based on the IDS storing the container information and identified in reference to the IDC list, when said secure container is used, in addition to the second processing section being performed.

30. (Withdrawn) A program providing medium, storing a program which comprises the steps of:

executing a content distribution process for performing content transaction management so that a content is secondarily distributed among a plurality of user devices; and

executing a personal authentication based on an IDC identified in reference to a IDC identifier list when a secure container is transmitted among the plurality of user devices, wherein the secure container contains the content encrypted by a content key, and container information including conditions set for a transaction of the content as well as the IDC identifier list serving as a list of the IDCs storing a template, each IDC serving as identification data of a target user for the content transaction.

31. (Cancelled).